Les attaques informatiques (virus, pirates...)

Les différents types d'attaques *:*

Le virus : Un virus est un bout de code de quelques octets (pour le rendre quasi invisible à "l'il nu") dont la fonction est destructrice ou très gênante.
Son but est de détruire une partie ou toutes les données de l'ordinateur, ou encore de rendre inutilisables certaines fonctions du PC. Il peut en outre ralentir certaines procédures. Son principe de fonctionnement diffère suivant les virus.

Les différents types de virus :

Le virus de zone amorce :

Un virus de zone damorce infecte la zone damorce des disques durs et des disquettes.
La zone damorce est la première partie du disque lue par l'ordinateur lors de son démarrage, elle contient les informations expliquant à l'ordinateur comment démarrer.

Pour être infecté, il faut avoir démarré sur une disquette, ou un disque amovible contenant le virus. Une fois la zone damorce de l'ordinateur infectée, ce virus se transmettra sur toute disquette ou support amovible inséré dans l'ordinateur.
La plupart des virus de zone damorce ne fonctionnent plus sous les nouveaux systèmes d'exploitation tels que Windows NT, Windows XP, 2000 car ils sont formatés en NTFS et non en FAT 32 (sauf si vous n'avez pas converti votre disque dur en NTFS).

Le virus DOS :

La plupart des virus fonctionnent sous le système d'exploitation DOS, ancien système d'exploitation de Microsoft avant Windows. Faites quand même attention car Windows exécute les programmes DOS sans aucun problème même si beaucoup de virus DOS n'arrivent pas à se reproduire l'orsquils sont exécutés par Windows. Un virus écrit sous DOS sera beaucoup plus petit en taille que son équivalent écrit sous Windows, déjà petit lui aussi !
Le virus Windows :

Les virus Windows fonctionnent sous Windows et peuvent donc infecter les programmes fonctionnant sous Windows. Le nombre de virus Windows est beaucoup plus réduit que le nombre de virus DOS, néanmoins ils sont considérés comme une plus grande menace que les virus DOS puisque la plupart des ordinateurs fonctionnent sous Windows.

Le virus Macro :

Les virus Macros sont la plus grande menace à ce jour, ils se propagent l'orsqun document Microsoft Word, Excel ou PowerPoint contaminé est exécuté. Une Macro est une série de commandes permettant d'effectuer des fonctions automatiquement au sein des applications Microsoft citées ci dessus. Le but du langage de macro est de pouvoir créer des raccourcis pour effectuer des fonctions courantes, par exemple en une touche enregistrer un document et ensuite l'imprimer.

Les Virus Macros se répandent très facilement. Louverture d'un document infecté va contaminer le document par défaut de l'application, et ensuite tous les documents qui seront ouverts par cette application. Les documents Word, Excel et PowerPoint étant les documents les plus souvent partagés au sein même d'une entreprise par exemple, ou envoyés par Internet, ceci explique la diffusion exponentielle de ces virus. Un conseil pour les éviter, Mettez un haut niveau de sécurité (outils, puis macros, puis sécurité, mettez ensuite haut).
Le virus polymorphe :

N'importe lequel des types de virus peut être polymorphe. Les virus polymorphes incluent un code spécial permettant de rendre chaque infection différente de la précédente. Ce changement constant rend la détection de ce type de virus compliqué. Souvent le code du virus change, mais l'action pour lequel il a été créé est toujours la même. Ces virus sont très difficiles à éliminer car ils trompent la vigilance de l'antivirus qui recherche une signature précise.
Beaucoup de virus polymorphes sont cryptés, en plus de leur changement de code. Le virus cryptera son code et ne le décryptera que l'orsquil doit infecter un nouveau fichier, le rendant encore plus difficile à détecter.
La meilleure protection contre les virus reste à avoir un bon antivirus régulièrement mis à jour (2 fois par mois), car un virus nouveau apparaît chaque jour et il existe toujours un risque de contamination même si vous avez mis votre antivirus à jour il y a un mois.

Le cheval de Troie :

Un cheval de Troie est un programme installé discrètement par un pirate sur votre ordinateur simulant une certaine action, mais faisant tout autre chose en réalité.
Le nom vient du fameux "Cheval de Troie", offert en cadeau pour la paie entre les Pays, mais qui avait en fait pour but de causer la ruine et la destruction de la ville ayant reçu ce cheval.
Un cheval de Troie sur un ordinateur est un programme exécutable qui est présenté comme ayant une action précise, généralement bénéfique pour l'ordinateur.
Mais lorsque ce programme est lancé, il va causer des actions plus ou moins graves sur votre ordinateur, comme supprimer des mots de passe, voler des mots de passe, envoyer des informations confidentielles au créateur du programme, formater votre disque dur...
Pour rechercher et éliminer d'éventuels chevaux de troie, vous pouvez télécharger The Cleaner ici:
http://www.moosoft.com

Les hoax ou "faux virus" :

Ces fausses alertes sont aussi sérieuses que les vrais virus, et malheureusement elles sont en constante augmentation.
Elles font perdre du temps et peuvent générer un doute quant à la vérité ou non du message.
Si vous recevez un message du type "si vous recevez un email avec comme sujet machin, effacez-le, ne l'ouvrez pas, il formatera votre disque dur", n'en tenez pas compte, supprimez le message et surtout ne l'envoyez pas à tout votre carnet d'adresses, cela ne fait qu'engorger le réseau.

Le ver :

Un Ver est un petit programme qui se copie d'ordinateur en ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme et ne peut donc l'infecter, il va simplement se copier d'ordinateur en ordinateur par l'intermédiaire d'un réseau comme Internet ou même par les lecteurs de disquettes, graveur, lecteur zip...
Le ver peut donc non seulement affecter un ordinateur, mais aussi dégrader les performances des réseaux. Comme un virus, le ver peut contenir une action nuisible qui peut être très grave comme le formatage de votre disque dur ou l'envoi de données confidentielles.
Le piratage en direct :

Le piratage en direct du micro pendant que vous êtes connecté à Internet est un véritable fléau. Le but des pirates est de supprimer ou de voler vos fichiers (on prend son plaisir ou on peut !).
La probabilité de ces attaques dépend du temps que vous passez sur Internet et de la configuration de votre ordinateur.
Depuis l'apparition de Windows, il y a un composant appelé NetBIOS. C'est un protocole destiné à faciliter le partage des dossiers et fichiers dans un réseau local. Mais si vous avez une connexion Internet,
Ce composant gênant permettra à un pirate d'accéder à vos dossiers partagés. Si vous n'avez pas de firewall, débarrassez vous en !
Avec Windows 98 ou millenium :
Cliquez avec le bouton droit sur voisinage réseau ou favoris réseau qui se trouve sur le bureau.
Cliquez sur propriétés. Si vous avez un modem RTC, vous y trouverez un composant nommé TCP/IP -> Carte d'accès réseau à distance.
Si vous avez l'ADSL ou le câble, ce composant s'appellera TCP/IP -> suivit du nom de votre carte Ethernet ou de votre modem.
Double cliquez dessus, puis, dans la fenêtre qui s'ouvre, allez dans l'onglet liens. Décochez les deux cases intitulées Client pour les réseaux Microsoft et Partage des fichiers et imprimantes pour les réseaux Microsoft.
Cliquez sur OK et redémarrez windows.
Avec Windows XP :

Cliquez sur démarrer, panneau de configuration, connexion réseau et Internet (ou connexions réseau).
Cliquez sur l'icône de votre connexion Internet avec le bouton droit et sélectionnez propriétés. Dans l'onglet général, sélectionnez protocole Internet TCP/IP, cliquez sur propriétés, puis avancées.
Activez l'onglet WINS, cochez la case Désactiver netBIOS avec TCP/IP, puis cliquez sur OK.